Vanessa R. Waldref
United States Attorney
Eastern District of Washington
Richard R. Barker
Assistant United States Attorney
Post Office Box 1494
Spokane, WA 99210-1494
Telephone: (509) 353-2767

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA, Plaintiff, v. RONALD CRAIG ILG (a/k/a "SCAR215"), Defendant.	2:21-CR-00049-WFN-1 UNITED STATES' INITIAL NOTICE OF EXPERT WITNESS AND RULE 16 SUMMARY

Plaintiff United States of America, by and through Vanessa R. Waldref, United States Attorney for the Eastern District of Washington, and Richard R. Barker, Assistant United States Attorney, respectfully submits the following Notice of Expert Witness and Rule 16 Summary.

This Notice of Expert Witness and Rule 16 Summary was prepared by the assigned Assistant United States Attorney and was neither written nor reviewed by any of the proposed experts referenced herein. Therefore, this written notice does not contain any adopted statements of the proposed expert witnesses and any questions from counsel should be derived from reports authored by the proposed expert rather than from this Notice of Expert Witness and Rule 16 Summary. The United States remains available to discuss with defense counsel any matters related to the expected testimony referenced in this Notice of Expert Witness and Rule 16 Summary. The United States also reserves the

right, and intends, to supplement this Notice of Expert Witnesses and Rule 16 Summary in the event that the United States obtains additional evidence not currently in its custody or control. In the event that the United States obtains any such additional evidence, it will provide such evidence and supplemental notice to the defense.

Notice of Lay and Expert Witnesses

This Notice of Expert Witness and Rule 16 Summary is meant to provide defense counsel with written notification pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G) relating to individuals who may be called as an expert witness at trial. Rule 16(a)(1)(G) requires the government to provide a written summary, which "describe[s] the witness's opinions, the bases and reasons for those opinions and the witness's qualifications."

The United States does not anticipate offering all of the proposed expert witness's testimony pursuant to Federal Rules of Evidence 702, 703, or 705.[1] Rather, although

[1] The Ninth Circuit has held that many observations which are common, yet still require a certain amount of expertise, can properly be characterized as lay opinion testimony, even when made by law enforcement personnel. *See United States v. Von Willie*, 59 F.3d 922, 929 (9th Cir. 1995) (police officer's testimony regarding nexus between drug trafficking and possession of weapons was admissible as lay witness opinion; "these observations are common enough and require such a limited amount of expertise, if any, that they can, indeed, be deemed lay witness opinion"); *see also* Fed. R. Evid. 701 (specifying that lay witness testimony "in the form of opinions or inferences" is permitted when "helpful to a clear understanding of the witness' testimony or the determination of a fact in issue"); *United States v. Hairston*, 64 F.3d 491, 493 (9th Cir. 1995) (testimony by federal agency employees of the Veterans Administration Medical Center regarding operations and ownership of funds properly admitted as lay opinion testimony under Rule 701, because employees were familiar with operations and handled the funds as part of their employment duties); *United States v. Munoz-Franco*, 487 F.3d

certain of the testimony referred to herein will contain technical aspects, much of the witnesses' testimony will be in their capacity as percipient witnesses, involve lay opinion testimony, be offered for other purposes, such as for authentication under Federal Rule of Evidence 901, or be introduced for the purpose of identifying materials recovered from computer media. *See, e.g.*, *United States v. Scott-Emuakpor*, 2000 WL 288443, at *12 (W.D. Mich. Jan. 25, 2000). Nevertheless, the United States makes these disclosures out of an abundance of caution in the event that the Court deems any of the testimony referenced herein to be expert testimony. Additionally, the United States intends to examine the witnesses referenced herein about the full extent of their background as set forth in each witness's curriculum vitae. The United States further intends to examine the witnesses about the full extent of any relevant reports referenced herein.

1. Cryptocurrency and Blockchain Expert

At the trial, the United States anticipates calling FBI Forensic Accountant Brandon Tabbal to testify as an expert on crypto currency and blockchain analysis. Forensic Accountant Tabbal's qualifications are set forth in his curriculum vitae, which has been provided to Defense under separate cover. *See* Bates 60000051.

Forensic Accountant Tabbal is anticipated to testify generally that cryptocurrency, a type of virtual currency, is a decentralized, peer-to peer, network-based medium of value or exchange that may be used as a substitute for fiat currency to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Examples of cryptocurrency are Bitcoin, Litecoin, and Ether. Cryptocurrency can exist digitally on the Internet, in an electronic storage device, or in cloud-based servers. Although not usually stored in any physical form, public, and private keys (described below) used to

---

25 (1st Cir. 2007) (bank officer properly testified under Rule 701 as a lay witness about the propriety of certain loans, due to his banking experience and particular knowledge about the loans in question).

transfer cryptocurrency from one person or place to another can be printed or written on a piece of paper or other tangible object.

Cryptocurrency can be exchanged directly person to person, through a cryptocurrency exchange, or through other intermediaries. Generally, cryptocurrency is not issued by any government, bank, or company; it is instead generated and controlled through computer software operating on a decentralized peer-to-peer network. Most cryptocurrencies have a "blockchain," which is a distributed public ledger, run by the decentralized network, containing an immutable and historical record of every transaction.

Forensic Accountant Tabbal is further anticipated to explain, as noted above, that Bitcoin is a type of cryptocurrency. Payments or transfers of value made with Bitcoin are recorded in the Bitcoin blockchain and thus are not maintained by any single administrator or entity. As mentioned above, individuals can acquire Bitcoin through exchanges (i.e., online companies which allow individuals to purchase or sell cryptocurrencies in exchange for fiat currencies or other cryptocurrencies). Individuals can also acquire Bitcoin from certain ATMs, or directly from other people.

Individuals can send and receive cryptocurrencies online using many types of electronic devices, including laptop computers, and smart phones. Even though the public addresses of those engaging in cryptocurrency transactions are recorded on a blockchain, the identities of the individuals or entities behind the public addresses are not recorded on these public ledgers. If, however, an individual or entity is linked to a public address, it may be possible to determine what transactions were conducted by that individual or entity. Bitcoin transactions are therefore sometimes described as "pseudonymous," meaning that they are partially anonymous. And while it's not completely anonymous, Bitcoin allows users to transfer funds more anonymously than would be possible through traditional banking and financial systems.

Forensic Accountant Tabbal is further expected to testify that cryptocurrency is stored in a virtual account called a wallet. Wallets are software programs that interface

with blockchains and generate and/or store public and private keys used to send and receive cryptocurrency. A public key or address is akin to a bank account number, and a private key is akin to a PIN number or password that allows a user the ability to access and transfer value associated with the public address or key. To conduct transactions on a blockchain, an individual must use the public address (or "public key") and the private address (or "private key"). A public address is represented as a case-sensitive string of letters and numbers, 25–26 characters long. Each public address is controlled and/or accessed through the use of a unique corresponding private key – the cryptographic equivalent of a password or PIN – needed to access the address. Only the holder of an address' private key can authorize any transfers of cryptocurrency from that address to another cryptocurrency address.

Although cryptocurrencies such as Bitcoin have legitimate uses, cryptocurrency is also used by individuals and organizations for criminal purposes such as money laundering and is an often used means of payment for illegal goods and services on hidden services websites operating on the Tor network. By maintaining multiple wallets, those who use cryptocurrency for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within the dark web marketplaces.

Forensic Accountant Tabbal is expected to explain that exchangers and users of cryptocurrencies store and transact their cryptocurrency in a number of ways, as wallet software can be housed in a variety of forms, including on a tangible, external device ("hardware wallet"), downloaded on a PC or laptop ("desktop wallet"), with an Internet-based cloud storage provider ("online wallet"), as a mobile application on a smartphone or tablet ("mobile wallet"), printed public and private keys ("paper wallet"), and as an online account associated with a cryptocurrency exchange. Because these desktop, mobile, and online wallets are electronic in nature, they are located on mobile devices (e.g., smart phones or tablets) or at websites that users can access via a computer, smart phone, or any device that can search the Internet. Moreover, hardware wallets are located on some type of external or removable media device, such as a USB thumb drive or other

commercially available device designed to store cryptocurrency. Paper wallets contain an address and a QR code with the public and private key embedded in the code. Paper wallet keys are not stored digitally.

Forensic Accountant Tabbal is expected to further explain that wallets can be backed up into, for example, paper printouts, USB drives, or CDs, and accessed through a "recovery seed" (random words strung together in a phrase) or a complex password. Additional security safeguards for cryptocurrency wallets can include two-factor authorization (such as a password and a phrase). As a general matter, individuals possessing cryptocurrencies often have safeguards in place to ensure that their cryptocurrencies become further secured in the event that their assets become potentially vulnerable to seizure and/or unauthorized transfer.

Forensic Accountant Tabbal is expected to testify that registered money transmitters are required by law to follow Bank Secrecy Act anti-money laundering ("AML") regulations, "Know Your Customer" ("KYC") protocols, and other verification procedures similar to those employed by traditional financial institutions. For example, registered cryptocurrency exchangers often require customers who want to open or maintain accounts on their exchange to provide their name, address, phone number, and the full bank account and routing numbers, which the customer is then able to link to an exchange account.

Some companies offer cryptocurrency wallet services, which allow users to download a digital wallet application onto their smart phone or other digital device. A user typically accesses the wallet application by inputting a user-generated PIN code or password. Users can store, receive, and transfer cryptocurrencies via the application; however, many of these companies do not store or otherwise have access to their users' funds or the private keys that are necessary to access users' wallet applications. Rather, the private keys are stored on the device on which the wallet application is installed (or any digital or physical backup private key that the user creates). As a result, these companies generally cannot assist in seizing or otherwise restraining their users'

cryptocurrency. Nevertheless, law enforcement could seize cryptocurrency from the user's wallet directly, such as by accessing the user's smart phone, accessing the wallet application, and transferring the cryptocurrency therein to a law enforcement-controlled wallet.

Forensic Accountant Tabbal is further anticipated to explain that where law enforcement has obtained the recovery seed for a wallet (see above), law enforcement may be able to use the recovery seed phrase to recover or reconstitute the wallet on a different digital device and subsequently transfer cryptocurrencies held within the new wallet to a law enforcement-controlled wallet. The recovery seed phrase is simply a condensed, encoded version of the private keys (described above), which can be decoded using a variety of different tools. This is analogous to unzipping a computer file or translating a document. There are several standardized seed phrase formats. The most common is Blockchain Implementation Protocol (BIP) 39. However, some wallet software programs – including a program named Electrum – use their own seed phrase formats. Several standalone tools (including open source tools) exist for viewing the private keys associated with a recovery seed phrase. Recovery seed phrases can also be decoded using the same version of the wallet software that was used to create them. For example, if agents locate an Electrum recovery seed phrase, agents can view the associated keys by importing that recovery seed phrase into a new Electrum wallet.

In addition to the background information set forth above, Forensic Accountant Tabbal is anticipated to further testify about the specific analysis he conducted in this case, including in his draft report dated January 27, 2022. Bates 60000052. As set forth in Forensic Accountant Tabbal's report, the FBI located a recovery seed phrase during a search of Defendant's home (biometric safe), luggage, and phone. The seed phrase was used to recover or reconstitute a specific Bitcoin wallet (hereafter the "Seed Phrase Wallet"). From that wallet, several Bitcoin payments were made to the Bitcoin Addresses associated with the Sinaloa dark website and the DBE dark website identified by the FBI during the investigation. Over 99% of the deposits into the Seed Phrase Wallet originated

from a combination of Defendant's Coinbase account, his Moon Pay account, and transactions conducted by Defendant at two different Bitcoin ATMs in Spokane, Washington. Forensic Accountant Tabbal is expected to further testify that Defendant funded and had control over the Seed Phrase Wallet during the times relevant to this investigation.[2]

2. Dark Web and the Tor Network

At trial, the United States anticipates calling FBI Special Agents Eric Yingling or Nathan Cocklin[3] as an expert to provide background information pertaining to the "Dark Web," which is otherwise known as the "Deep Web" of the Internet. Special Agent Yingling is a Supervisory Special Agent (SSA) within the FBI's Virtual Assets Exploitation Unit (VAXU) at FBI Headquarters. Special Agent Cocklin is the Unit Chief for the Hi-Tech Organized Crime Unit for the FBI in Washington, D.C. Both have extensive experience investigating criminal activity occurring on the Dark Web.

SSA Yingling worked on a variety of violations to include complex financial crimes, Dark Web marketplaces, Dark Web narcotics traffickers, and virtual currency money laundering facilitators. SSA Yingling also helped to establish the FBI's High Tech Organized Crime Unit and the subsequent Joint Criminal Opioid & Darkweb Enforcement Team (JCODE). He has worked with Europols Darkweb Team and has provided trainings to law enforcement agencies around the globe.

---

[2] Forensic Accountant Tabbal is further examining additional transactions made in connection with the payments over the dark web to harm Victim 1 and to pay a dark web hacker to access Victim 2's phone and other electronic devices. The United States will supplement its expert notice with any additional information regarding these payments.

[3] Depending on witness availability, the United States may call Special Agent Cocklin. Assuming a trial date in September 2022, the United States, at this time, anticipates calling SSA Yingling. If Special Agent Cocklin is to be called, the United States will provide supplemental notice further detailing Special Agent Cocklin's background.

SSA Yingling has worked collaborative Dark Web cases with numerous international law enforcement entities and domestic intelligence partners. Since 2015, SSA Yingling has been the case agent on a number of successfully prosecuted cases involving actors across the Dark Web ecosystem to include dark web marketplaces, vendors, and money launderers.

At trial, either Special Agent Yingling or Cocklin is anticipated to explain how the Dark Web is accessed – e.g., by using anonymizing software or an application called a "darknet" to access content and websites. Within the Dark Web, criminal marketplaces operate, allowing individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet (sometimes called the "clear web" or simply the "web"). These online market websites use a variety of technologies, including the Tor network (explained further below) and other encryption technologies, to ensure communications and transactions are shielded from interception and monitoring. Well-known Dark Web marketplaces, also called Hidden Services, such as Silk Road, AlphaBay, and Hansa (all of which have since been shut down by law enforcement), operated similarly to clear web commercial websites such as Amazon and eBay, but offered illicit goods and services.

Special Agent Yingling or Cocklin is expected to testify that "Vendors" are the Dark Web's sellers of goods and services, often of an illicit nature, and they do so through the creation and operation of "vendor accounts" on Dark Web marketplaces. Customers, meanwhile, operate "customer accounts." Vendor and customer accounts are not identified by numbers, but rather monikers or "handles," much like the username a person would use on a clear web site. If a moniker on a particular marketplace has not already been registered by another user, vendors and customers can use the same moniker across multiple marketplaces, and based on seller and customer reviews, can become well known as "trusted" vendors or customers. It is also possible for the same person to operate multiple customer accounts and multiple vendor accounts at the same time. For example, a person could have a vendor account that he or she uses to sell illegal goods on a Dark

Web marketplace in exchange for cryptocurrency; that same vendor could also have a different customer account that he or she uses to exchange cryptocurrency earned from vendor sales for fiat currency.

Special Agent Yingling or Cocklin is expected to further testify that the "Tor network," or simply "Tor" (an abbreviation for "The Onion Router"), is a special network of computers on the Internet, distributed around the world, designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network, and, thereby, the locations and identities of the network's users. Tor also enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services" on the Tor network. Such hidden services operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a browser known as the "Tor Browser," which is designed to access the Tor network. Examples of hidden services websites are the aforementioned AlphaBay and Hansa. Tor is available on cellphones using the Android and Apple operating systems by installing an application that puts a Tor-enabled internet browser on a user's cellphone, which then routes the phone's IP address through different servers all over the world, making it extremely difficult to track.

At trial, the United States may seek to introduce demonstrative exhibits describing and illustrating how the dark web operates along with demonstratives relating to the Tor Browser. Such exhibits will be provided during the normal course of discovery.[4]

[4] Depending on the timing of the trial, scheduling, and availability, the United States reserves the right to supplement this notice with another similar witness as necessary. In the event that another expert witness will be testifying rather than Special Agents Yingling or Cocklin, the United States will provide that witness's background information, upon receipt of said information.

3. Handwriting Expert

The United States anticipates calling Gabriel D. Watts, who works in the FBI's Questioned Documents Unit, to testify regarding handwriting analysis in this case. Mr. Watts, whose expertise is handwriting examination and comparison, is expected to testify consistent with his report dated December 2, 2021. Bates 00000467.

At trial, Mr. Watts will describe the FBI's Questioned Documents Unit and explain the methodology used to assess handwriting. Mr. Watts is expected to testify that the methodology utilized when conducting an initial assessment of documentary evidence involves an examination of the submitted evidence to observe and note features of the submitted item(s), record characteristics which may be important for future examinations, assess the feasibility of the requested examinations, and identify other potentially probative examinations. This analysis begins with a visual examination using ambient lighting. If necessary, microscopic, optical, and/or electrostatic analysis of the submitted item(s) and the use of additional specialized equipment, lighting, and/or reference materials may be employed. When applicable, these methods and techniques are utilized to assess the various substrates, writing, machine printing, mechanical impressions, indentations, watermarks, writing/printing mediums, and/or other documentary components of the submitted evidence. When conducting these types of initial assessments and physical examinations of the evidence, at a minimum, any probative characteristics observed that may be altered or destroyed by any other examinations (e.g. latent processing) must be recorded. The examination records also may be used in future comparisons.

Mr. Watts is expected to testify generally that the following equipment, methods, and techniques may be used during the initial assessment of the submitted evidence:

- Electrostatic Detection Apparatus (ESDA)
- Video Spectral Comparator (VSC)
- Hyperspectral Imaging (HSI Examiner)

- Digital Microscopy
- Stereoscope/other microscopy
- Various forms of specialized lighting
- 3M Glare-Stop polarizing filters of various sizes
- Various measuring devices such as calipers, rulers, etc.
- Various reference materials and/or software

Mr. Watts is further expected to testify that following the initial assessment, the examination may then proceed to an "Evaluation" phase. In instances when examinations do not continue into a comparison procedure, results of the initial assessment deemed probative, indented writing results, and/or watermark results will be reported. These results may include, but are not limited to, the following information (as applicable):

- Writing medium(s) and/or printing process(es) used to produce an item
- Presence/absence of watermark and/or manufacturer's information
- Self-adhesive/moisture-activated properties of an item
- Presence/absence of indented writing and possible interpretation of the indentations
- Suitability of an item for future examinations
- Request for additional items
- Any additional observations and assessments that are made and recorded for future examinations

Following the evaluation, Mr. Watts's examination proceeds to a "verification and review" phase. Verifications are performed in instances when a printing process or an interpretation of the content of the indented writing is included in the results of examinations section of the report. Verifications ensure the accuracy of these examinations while additional reviews ensure the appropriate examinations have been conducted, the examiner's conclusions are consistent with technical notes, the technical

notes contain sufficient supporting data and are within the limits of the discipline, and all records conform to Laboratory standards.

Mr. Watts is further expected to testify regarding certain factors that may affect the examination process and/or the results rendered. These limitations include the following:

- Prior destructive examinations
- Non-original writing
- Insufficient quantity of original material
- Insufficient quantity of physical characteristics/class characteristics associated with the item(s)
- Limited/Lack of comparability
- Oversized/bulky items
- Poor condition of the material

Mr. Watts is further expected to speak to the comparison methodology used when conducted handwriting analysis. That methodology is set forth in Mr. Watts's report dated December 1, 2021, and includes examination of certain characteristics, including: beginning and ending strokes, baseline features, height relationships, slant, spacing, and line quality. Handwriting samples are compared side-by-side. The numerous characteristics exhibited in the writing between the items are then examined to determine the similarities, differences, and limitations, if present.

Based on the significance and combination of the characteristics observed, the examiner may then make a conclusion. In this case, Mr. Watts concluded that there was *support for a common source*. Specifically, as set forth in his report, Mr. Watts stated that while "[a] source identification could not be reached due to the presence of unexplained characteristics, limited clarity and detail, and limited comparable known writing submitted for examination," there were "characteristics in common" indicating Defendant prepared the writings submitted for review. Mr. Watts's curriculum vitae,

which is hereby incorporated by reference, has been provided through discovery in Bates 60000004.

Please note the United States is evaluating whether to conduct additional handwriting review, including comparison with additional known samples from Defendant. The additional samples were provided to the FBI by Defendant's ex-wife on January 31, 2021. If such review is conducted, the United States will notify Defendant's counsel of the results of such review.

4. Computer Forensics

The United States anticipates calling FBI Forensic Examiner John Powers and/or Forensic Examiner Kevin Hall from the FBI's Computer Forensics Laboratory Computer Analysis Response Team ("CART") Program to testify at trial. Members of the FBI's CART Program, including Messrs. Powers and/or Hall, are expected to testify regarding physical and file system extractions as well as images from various electronic devices examined in this case, including:

(1) iPhone Xs Max, belonging to Witness 1;

(2) Samsung Galaxy S10e, belonging to Victim 2;

(3) Samsung Galaxy, belonging to Defendant;

(4) ZTE cellular phone model Z433, recovered from the search of Defendant's residence;

(5) Samsung tablet, serial number RF2F11WVWNK;

(6) Samsung tablet, serial number RF2DA0BMRAP;

(7) Samsung tablet, model SCH-1705, IMEI 990004465137507;

(8) Sony Vaio laptop, serial number 545107600029319; and

(9) HP Laptop, serial number 5CD05282J2

The government anticipates that CART examiners will testify that the extraction from the cell phones described above were recovered using a Physical Analyzer (PA), which generated a Universal Forensic Extraction Device (UFED) report. The respective

examiners who performed these extractions are expected to testify that they prepared the Cellebrite Extraction to be reviewed through a reader executable file, so that the case agents and analysts could review information recovered for evidentiary value. Mesers. Powers and/or Hall are expected to further testify regarding the images of Defendant's other electronic devices, as well as the manner that these images were obtained and analyzed.

With respect to the generation of the extractions and images disclosed through discovery, the government emphasizes that Examiners Powers and/or Hall will be offered only for their technical and specialized knowledge in the area of electronic device examination, not, for example, for expertise in the field of hardware or software development. *See United States v. Berry*, 318 Fed. Appx. 569, 570 (9th Cir. 2009) (a forensic examiner who "simply testified to what he found on the hard drive of [the defendant's] computer, without expressing an opinion that required specialized knowledge or offering insight beyond common understanding" was a fact witness, not an expert); *United States v. Scott Emuakpor*, 2000 WL 288443, *12, (W. D. Mich. Jan. 25, 2000) ("The question before the Court at this time is not whether these witnesses have the expertise, for example, to develop sophisticated software programs. The question is whether they have the skill to find out what is on a hard drive or a zip drive. Apparently, they have this skill because they determined what was on the drives.").

In addition to how the extractions and images were obtained, Forensic Examiners Powers and/or Hall are anticipated to testify regarding their further analysis of various devices belonging to Defendant, including any indicia, or lack thereof, of any unauthorized access to Defendant's electronic devices. The United States anticipates supplementing this notice upon the completion of Forensic Examiners Powers's and Hall's ongoing analysis and will provide any supplement to Defense upon receipt. Forensic Examiner Powers's curriculum vitae is set forth in Bates 60000050, which is incorporated herein by reference. Depending on witness availability and scheduling,

Examiner Hall's CV will be provided in the event Examiner Powers is not available for trial.

5. Biometrics

The United States anticipates that Special Agents David DiBartolo, Eric Barker, and/or Ryan Butler will testify at trial about two biometric safes located within Defendant's home during the execution of a search warrant on April 11, 2021. One of the safes was taken as evidence pursuant to separate search warrant on May 14, 2021. While Special Agents DiBartolo, Barker, and Butler will not be qualified as experts at trial, the United States anticipates that one or both will offer lay witness testimony regarding their training and experience with biometric devices. Based on this training and experience, users of a device that offer biometric unlocking functionality – e.g., by storing one or more fingerprints in the device's internal computer – often enable such functionality for convenience and security. Where a person has a biometric device in his or her home or place of business, that person is more likely to have access to the device. A user, whose fingerprint or other biometric data opens device, can be said to have access, possession, and control over the contents of that device – in this case, the two biometric safes. Special Agent Barker and/or Butler is anticipated to testify at trial that Defendant depressed his finger on the two biometric safes described herein. The safes opened when Defendant depressed his fingerprint on the biometric devices.

Should the Court or Defense have any questions regarding Special Agents DiBartolo, Barker, and Buter's training, experience, or otherwise believe additional notice is required, please let us know as soon as possible, by including the factual and legal basis for requiring Special Agents DiBartolo, Barker, and/or Butler to be qualified as experts.

Reciprocity

Having provided notice and summaries pursuant to Rule 16(a)(1)(G), the United States hereby formally requests disclosure pursuant to Rule 16(b)(1)(C) of any expert testimony that the defense intends to offer. To date, no such notice has been received.

Conclusion

The United States respectfully submits that the foregoing summarizes the expected expert testimony (to the extent that any such testimony is not considered lay opinion testimony or otherwise not expert testimony) that will assist the trier of fact in understanding the evidence and determining material facts at issue. The United States again reserves the right to supplement this Notice given the technological nature of the case, scheduling conflicts, and the ongoing review of evidence. If the Court or counsel believe this Notice and these Summaries are deficient under Rule 16, the United States requests notice and an opportunity to be heard on these issues prior to trial, in an effort to streamline trial in an efficient manner.

Dated this 4th day of February 2022

Vanessa R. Waldref
United States Attorney

s/ Richard R. Barker
Richard R. Barker
Assistant United States Attorney

CERTIFICATION

I hereby certify that on February 4, 2021, I electronically filed the foregoing with the Clerk of the Court and counsel of record using the CM/ECF System.

s/Richard R. Barker
Richard R. Barker
Assistant United States Attorney